IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. PHILLIP R. DURACHINSKY, Defendant.	SUPERSEDING INDICTMENT JUDGE SOLOMON OLIVER, JR. CASE NO. 1:18CR00022 Title 18, United States Code, Sections 1028A(a)(1), 1030(a)(2), (a)(3), (a)(5)(A), (c)(2)(A), (c)(4)(B)(i), 1343, 2251(a) and (e), 2511(1)(b) and (4)(a), and 2

GENERAL ALLEGATIONS

At all times material herein:

1. From in or around 2003 through on or about January 20, 2017, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY engaged in a scheme to access protected computers without permission.

2. During his more than thirteen years of accessing protected computers without the appropriate authorizations, Defendant accessed protected computers owned by local, state and federal governments, a police department, schools, companies and individuals.

3. Defendant developed computer malware, later named "Fruitfly," and wrote variants capable of infecting computers running macOS and Windows operating systems.

4. Defendant installed the Fruitfly malware on thousands of computers ("Fruitfly victims").

5. The Fruitfly malware gave Defendant the ability to control a Fruitfly victim's computer by, among other things, accessing stored data, uploading files to a Fruitfly victim's computer, taking and downloading screenshots, logging a user's keystrokes and turning on the camera and microphone to surreptitiously record images and audio.

6. In certain cases, the Fruitfly malware alerted Defendant if a user of an infected computer typed certain words associated with pornography. Defendant used the Fruitfly malware to watch and listen to Fruitfly victims without their knowledge or permission. He saved millions of images and regularly kept detailed notes of what he observed.

7. Defendant developed a control panel for the Fruitfly malware that ran on a computer in a residence in the Northern District of Ohio, Eastern Division. The control panel allowed Defendant to manipulate computers infected with the Fruitfly malware and had a visual interface that allowed Defendant to view live images and data from several infected computers simultaneously.

8. Defendant used his access to Fruitfly victims' computers to collect and save personal data from Fruitfly victims including tax records, medical records, photographs, internet searches performed, banking records and potentially embarrassing communications and data.

9. Defendant used the Fruitfly malware to obtain Fruitfly victims' usernames and passwords to third-party websites. Defendant used these stolen credentials to access and download information from these third-party websites including photographs, emails and potentially embarrassing communications and data.

10. Minor # 1 refers to a female child, whose identity is known to the Grand Jury and who was born in 1994.

11. Minor # 2 refers to a male child, whose identity is known to the Grand Jury and who was born in 1996.

12. Minor # 3 refers to a female child, whose identity is known to the Grand Jury and who was born in 1999.

COUNTS 1 - 5
(Intentional Damage to a Protected Computer
18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)(i) ((c)(4)(A)(i)(I) and (VI))

The Grand Jury charges:

13. The General Allegations in paragraphs 1 through 12 of this Superseding Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

14. On or about each of the dates set forth below, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct intentionally caused damage without authorization to a protected computer, and the offense caused (a) damage affecting 10 or more protected computers during a one-year period, and (b) loss to 1 or more persons during a one-year period resulting from a related course of conduct affecting 1 or more protected computers, aggregating at least $5,000, each transmission constituting a separate count:

Count	**Date**	**Computer(s)** [1]
1	September 6, 2013	R*****-B****-MacBook-Air-3
2	January 25, 2014	Z****-iMac

[1] As used throughout this indictment, some characters in the name of computers were replaced with asterisks in order to anonymize the victims' names.

Count	Date	Computer(s) [1]
3	August 30, 2014	CDB-Home-iMac
4	February 24, 2014	A*******-Computer
5	December 22, 2012	bcss-iMac-3

All in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B)(i) ((c)(4)(A)(i)(I) and (VI)).

COUNTS 6 - 10
(Accessing Protected Computer(s), 18 U.S.C. §§ 1030(a)(2) and (c)(2)(A))

The Grand Jury further charges:

15. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

16. On or about each of the dates set forth below, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally accessed one or more computers without authorization and thereby obtained information from one or more protected computers,

Count	Date	Computer(s)
6	September 6, 2013	R*****-B****-MacBook-Air-3
7	January 25, 2014	Z****-iMac
8	August 30, 2014	CDB-Home-iMac
9	February 24, 2014	A*******-Computer
10	December 22, 2012	bcss-iMac-3

All in violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(A).

COUNT 11
(Sexual Exploitation of a Child, 18 U.S.C. §§ 2251(a) and (e))

The Grand Jury further charges:

17. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

18. From on or about August 23, 2011, through on or about January 13, 2012, in the Northern District of Ohio, and elsewhere, Defendant PHILLIP R. DURACHINSKY did use and attempt to use a minor, Minor #1, to engage in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2), for the purpose of producing a visual depiction of such conduct, knowing and having reason to know that such visual depiction would be transported in and affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 2251(a) and (e).

COUNT 12
(Sexual Exploitation of a Child, 18 U.S.C. §§ 2251(a) and (e))

The Grand Jury further charges:

19. The General Allegations of paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

20. From on or about November 26, 2011, through on or about April 5, 2014, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY did use and attempt to use a minor, Minor #2, to engage in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2), for the purpose of producing a visual depiction of such conduct, knowing and having reason to know that such visual depiction would be transported in and affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 2251(a) and (e).

COUNT 13
(Sexual Exploitation of a Child, 18 U.S.C. §§ 2251(a) and (e))

The Grand Jury further charges:

21. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

22. From on or about April 8, 2012, through on or about January 13, 2016, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY did use and attempt to use a minor, Minor #3, to engage in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2), for the purpose of producing a visual depiction of such conduct, knowing and having reason to know that such visual depiction would be transported in and affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 2251(a) and (e).

COUNTS 14 - 26
(Wire Fraud, 18 U.S.C. §§ 1343 and 2)

The Grand Jury further charges:

23. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

24. In order to operate the Fruitfly malware, Defendant PHILLIP R. DURACHINSKY required access to the computers, storage, and internet bandwidth of other individuals and entities infected by or with the Fruitfly malware without their permission or authorization. Defendant required these facilities to, among other things, obfuscate his involvement in operating the Fruitfly malware, provide storage space for the images and files the Fruitfly malware generated, and provide sufficient bandwidth to support the vast amount of information created by the Fruitfly malware.

STATUTORY VIOLATION

25. From in or around August 14, 2011, through on or about January 20, 2017, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant devised and intended to devise a scheme and artifice to defraud Fruitfly victims and others, and to obtain money and property, to wit: computer processing power, computer storage, and internet bandwidth and connections, among other things, by means of materially false and fraudulent pretenses, representations, and promises.

26. It was part of the scheme that:

a) Defendant obtained and used user credentials and passwords for certain computers infected by the Fruitfly malware to create virtual machines on those Fruitfly victims' computers.

b) Defendant used the computing power of and infrastructure associated with certain Fruitfly victims' computers to spread the Fruitfly malware across the Internet.

c) Defendant used certain Fruitfly victims' computers to access sufficient bandwidth to allow the Fruitfly malware to infect protected computers in the Northern District of Ohio, Eastern Division, and elsewhere.

d) Defendant instructed the Fruitfly malware to direct Fruitfly victims' computers to report back and, thereafter, send images and files to certain other Fruitfly victims' computers to create repositories of data obtained by the Fruitfly malware. Defendant then remotely accessed these repositories to determine what materials he wanted to preserve in other locations.

e) Defendant created storage containers on certain Fruitfly victims' computers to store and process images and files obtained from other Fruitfly victims.

f) Defendant used certain Fruitfly victims' computers to create proxy networks and servers that obfuscated and concealed his role in operating the Fruitfly malware.

27. For the purposes of executing and attempting to execute said scheme and artifice to defraud the Fruitfly victims, and to obtain money and property by means of false and fraudulent pretenses, representations, and promises, and attempting to do so, transmitted and caused to be transmitted, by means of wire communications in interstate and foreign commerce, the signals and sounds described below for each count, each transmission constituting a separate count, to wit: various computer program commands and signals between Defendant and various computers in the Fruitfly network, each transmission constituting a separate count of this Indictment, as set forth below:

COUNT	APPROXIMATE DATE	DESCRIPTION OF WIRES
14	April 22, 2016	Communications and commands sent via the internet from a computer in the Northern District of Ohio to a server in Nevada, redirecting Fruitfly victim data to a computer lawfully controlled by C.B.
15	June 13, 2016	Communications and commands sent via the internet from a computer in the Northern District of Ohio to a server in Nevada, redirecting Fruitfly victim data to a computer lawfully controlled by C.B.
16	July 8, 2016	Communications and commands sent via the internet from a computer in the Northern District of Ohio to a server in Nevada, redirecting Fruitfly victim data to a computer lawfully controlled by Z.S.
17	July 9, 2016	Communications and commands sent via the internet from a computer in the Northern District of Ohio to a server in Nevada, redirecting Fruitfly victim data to a computer lawfully controlled by C.B.
18	July 12, 2016	Communications and commands sent via the internet from a computer in the Northern District of Ohio to a server in Nevada, redirecting Fruitfly victim data to a computer lawfully controlled by Z.S.

COUNT	APPROXIMATE DATE	DESCRIPTION OF WIRES
19	August 5, 2016	Communications and commands sent via the internet via a computer in the Northern District of Ohio directing Z.S.'s computer in California to attempt to decrypt or "crack" the password of an Office document.
20	August 5, 2016	Communications and commands sent via the internet via a computer in the Northern District of Ohio directing Z.S.'s computer in California to attempt to decrypt or "crack" the password of an Apple OSX Keychain.
21	August 23, 2016	Communications and commands sent via the internet via a computer in the Northern District of Ohio directing Z.S.'s computer to attempt to decrypt or "crack" the password of an Apple OSX Keychain.
22	December 31, 2016	Communications and commands sent via the internet via a computer in the Northern District of Ohio directing W.M.'s computer in California to attempt to decrypt or "crack" the password of an Apple OSX Keychain.
23	January 3, 2017	Communications and commands sent via the internet via a computer in the Northern District of Ohio directing W.M.'s computer in California to attempt to decrypt or "crack" the passwords of four email addresses.
24	January 14, 2017	Communications and commands sent via the internet via a computer in the Northern District of Ohio directing W.M.'s computer in California to attempt to decrypt or "crack" the password of an Apple OSX Keychain.
25	January 17, 2017	Communications and commands sent via the internet from a computer in the Northern District of Ohio to a server in Nevada, redirecting Fruitfly victim data to a computer lawfully controlled by W.M.
26	January 18, 2017	Communications and commands sent via the internet from a computer in the Northern District of Ohio to a server in Nevada, redirecting Fruitfly victim data to a computer lawfully controlled by W.M.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS 27 - 30
(Aggravated Identify Theft, 18 U.S.C. § 1028A(a)(1))

The Grand Jury further charges:

28. The General Allegations in paragraphs 1 through 12 and paragraph 24 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

29. On or about the dates listed below, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY did knowingly transfer, possess and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit: Wire Fraud, in violation of Title 18, United States Code, Section 1343, knowing that the means of identification belonged to another actual person on or about the dates set forth below:

COUNT	MEANS OF IDENTIFICATION	APPROXIMATE DATES
27	Username and Password for C.B.	August 20, 2014
28	Username and Password for C.B.	August 22, 2014
29	Username and Password for Z.S.	September 7, 2014
30	Username and Password for W.M.	March 29, 2015

All in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT 31
(Accessing Government Computer Without Authorization,
18 U.S.C. §§ 1030(a)(3) and (c)(2)(A))

The Grand Jury further charges:

30. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

31. Between on or about May 21, 2014, and on or about December 19, 2016, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY did intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, access such a computer of that department and agency that was exclusively for the use of the Government of the United States, and such conduct affected that use by and for the Government of the United States, namely a computer owned and operated exclusively by a subsidiary of the U.S. Department of Energy, an agency of the United States, in violation of Title 18, United States Code, Sections 1030(a)(3) and (c)(2)(A).

COUNT 32
(Illegal Wiretap, 18 U.S.C. §§ 2511(1)(b) and (4)(a))

The Grand Jury further charges:

32. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

33. On or about June 25, 2013, at approximately 2:25 p.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmitted a signal through a wire communication to intercept an oral communication of M.M. and an unknown female, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

COUNT 33
(Illegal Wiretap, 18 U.S.C. §§ 2511(1)(b) and (4)(a))

The Grand Jury further charges:

34. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

35. On or about June 23, 2014, between approximately 11:40 a.m. and 11:56 a.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmitted a signal through a wire communication to intercept an oral communication of J.P. and an unknown male, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

COUNT 34
(Illegal Wiretap, 18 U.S.C. §§ 2511(1)(b) and (4)(a))

The Grand Jury further charges:

36. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

37. On or about July 23, 2014, between approximately 7:54 p.m. and 7:57 p.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmitted a signal through a wire communication to intercept an oral communication of C.A. and an unknown male, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

COUNT 35
(Illegal Wiretap, 18 U.S.C. §§ 2511(1)(b) and (4)(a))

The Grand Jury further charges:

38. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

39. On or about March 14, 2015, between approximately 12:20 p.m. and 12:34 p.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmitted a signal through a wire

communication to intercept an oral communication of R.B. and an unknown female, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

COUNT 36
(Illegal Wiretap, 18 U.S.C. § 2511(1)(b) and (4)(a))

The Grand Jury further charges:

40. The General Allegations in paragraphs 1 through 12 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

41. On or about April 11, 2015, between approximately 2:21 p.m. and 2:26 p.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmitted a signal through a wire communication to intercept an oral communication of R.B. and an unknown female, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

FORFEITURE

The Grand Jury further charges:

42. The allegations of Counts 1 through 26 and 31 through 36 are hereby realleged and incorporated herein by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 982(a)(2)(B); Title 18, United States Code, Section 2253(a)(2); Title 18, United States Code, Section 2253(a)(3); Title 18, United States Code, Section 981(a)(1)(C); Title 28, United States Code, Section 2461(c); Title 18, United States Code, Section 1028(b)(5); Title 18, United States Code, Section 2513; and Title 28, United States Code, Section 2461(c). As a result of the foregoing offenses, Defendant PHILLIP R. DURACHINSKY shall forfeit the following to the United States:

a. All property constituting, or derived from, proceeds he obtained directly or indirectly as a result of the violations charged in Counts 1 through 5, 6 through 10, and 31.

b. All property, real or personal, constituting or traceable to gross profits or other proceeds obtained from the violation charged in Counts 11 through 13; and any property real or personal, used or intended to be used, to commit or to promote the commission of the violation charged in Counts 11 through 13 and any property traceable to such property.

c. All property, real or personal, which constitutes or is derived from proceeds traceable to the violations charged in Counts 14 through 26.

d. Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in the violations charged in Counts 32 through 36.

A TRUE BILL.

Original document - Signatures on file with the Clerk of Courts, pursuant to the E-Government Act of 2002.